Wymiana komunikatów edig@s z Polską Spółką Gazownictwa sp. z o.o. w oparciu o standard AS4

# Procedura przyłączenia nowego partnera

Prosimy o wysłanie wiadomości na adres nominacje.pomoc@psgaz.pl, w której zostaną przekazane następujące informacje dotyczące przyłączanego partnera:

1. **Adres IP**, z którego będą wysyłane komunikaty AS4 do PSG (wychodzący) i do którego będą wysyłane komunikaty od PSG (przychodzący), w celu odblokowania połączenia między serwerami AS4 przez sieć Internet. Jeśli adresów jest kilka należy je podać, z zaznaczeniem które są wychodzące, a które przychodzące.
2. **Adres URL** wraz z portem, na który będą miały być przesyłane dokumenty edig@s – adres produkcyjny i (jeśli istnieje) testowy.
3. **Kod EIC**.
4. **Certyfikaty** z kluczem publicznym, które będą używane w komunikacji AS4.
Certyfikat z kluczem publicznym używany jest do sprawdzenia podpisu cyfrowego otrzymanej wiadomości, szyfrowania wysyłanego dokumentu edig@s oraz weryfikacji szyfrowania SSL/TLS podczas wysyłaniu. Część prywatna certyfikatu (klucz prywatny, który należy chronić przed ujawnieniem) używana jest do podpisu wiadomości, deszyfrowania dokumentu edig@s i szyfrowania połączenia SSL/TLS.

Po przesłaniu kompletu powyższych informacji i pomyślnej weryfikacji partnera Polska Spółka Gazownictwa sp. z o.o. odpowie również przesyłając informacje z punktów 1-4 jej dotyczące.

Następnie po stronie PSG zdefiniowany zostanie P-Mode (Processing mode) w instancji testowej oprogramowania AS4 w celu powołania kanału przesyłania dokumentów między stronami, co pozwoli na przetestowanie połączenia AS4 poprzez przesłanie testowego pliku w obie strony.

# Szczegóły techniczne komunikacji AS4

Wersja dokumentów edig@s: 4.0 lub 5.1 (XML)

Wymieniane dokumenty edig@s: przyjmowanie NOMINT, odpowiadanie ACKNOW i NOMRES

Wzorzec komunikacji AS4: One-Way/Push

Połączenie: HTTPS (HTTP + TLS) port 443

Wersja TLS: 1.2

Stosowane certyfikaty:

* certyfikat SSL do zabezpieczania łączności HTTPS
* certyfikat AS4 do podpisywania wiadomości i szyfrowania przesyłanego pliku (ew. może być ten sam co certyfikat SSL)

# Ogólna specyfikacja certyfikatów

* Wersja certyfikatu: V3
* Algorytm podpisu: sha256RSA
* Ważność certyfikatu: preferowane 3 lata
* Składowe pola „Podmiot”:
	+ Country Name (C) – kod kraju, należy wpisać dużymi literami, np. „PL”,
	+ Organization Name (O) – pełna nazwa firmy,
	+ Organizational Unit Name (OU) – nazwa komórki firmy np. „IT”,
	+ Common Name (CN) – dla certyfikatu SSL należy podać adres domenowy lub nr IP serwera AS4 np. as4.mojafirma.pl lub 111.222.3.4. Jeżeli będzie to certyfikat typu Wildcard to wpisujemy np. \*.mojafirma.pl. Dla certyfikatu podpisu i szyfrowania wiadomości można wpisać kod EIC organizacji.
* Klucz publiczny: RSA (2048 bit)

# Wartości dla P-Mode

1. [Agreement]: http://entsog.eu/communication/agreements/<EIC\_Party\_A>/<EIC\_Party\_B>/<version>, gdzie kody EIC są posortowane alfabetycznie, a wersja początkowo przyjmuje wartość 1
2. [MEP]: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay
3. [MEPBinding]: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push
4. [Initiator.Party], [Responder.Party]: kod EIC
5. [Initiator.Role], [Responder.Role]: PSG przyjmuje rolę ZSO, podmiot przyłączający ZSH
6. [Service]: wartość produkcyjna A06, wartość testowa http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service
7. [Action]: wartość produkcyjna http://docs.oasis-open.org/ebxml-msg/as4/200902/action (domyślna), wartość testowa http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test
8. [Security.X509.Sign]: True
9. [Security.X509.Signature.HashFunction]: http://www.w3.org/2001/04/xmlenc#sha256
10. [Security.X509.Signature.Algorithm]: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
11. [Security.X509.Encryption.Encrypt]: True
12. [Security.X509.Encryption.Algorithm]: preferowane http://www.w3.org/2009/xmlenc11#aes128-gcm, dopuszczone http://www.w3.org/2001/04/xmlenc#aes128-cbc
13. [Security.X509.Encryption.MinimalStrength]: 128
14. [Security.SendReceipt.NonRepudiation]: True
15. [PayloadService.CompressionType]: application/gzip, dopuszczony również brak kompresji
16. Algorytm szyfrowania klucza: preferowane http://www.w3.org/2009/xmlenc11#rsa-oaep wraz z http://www.w3.org/2009/xmlenc11#mgf1sha256 i http://www.w3.org/2001/04/xmlenc#sha256, dopuszczone http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p
17. [SecurityTokenReference]: BinarySecurityToken (X509v3, X509PKIPathv1 lub X509IssuerSerial)

# O protokole AS4

Protokół AS4 (Applicability Statement 4) to standard opisujący bezpieczne i niezawodne przesyłanie komunikatów przez publiczną sieć Internet. Protokół ten bazuje na powszechnie znanych i sprawdzonych rozwiązaniach, takich jak protokoły HTTP, TLS, SOAP oraz usługach sieciowych (web service). Reprezentuje otwarty standard wymiany danych typu B2B opisany w specyfikacji OASIS ebMS 3.0. Elementami odpowiedzialnymi za bezpieczeństwo i wiarygodność przesyłanych danych są podpisy cyfrowe oraz mechanizmy szyfrujące (WS-security).

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.pdf>

# Implementacja protokołu AS4 w systemach przesyłowych gazu

<https://www.entsog.eu/sites/default/files/2019-05/INT0488-161115%20AS4%20Usage%20Profile_Rev_3.6_clean_final.pdf>

# Używane oprogramowanie AS4

<https://www.tel-ster.pl/index.php/telcomm/o-telcomm>